

## AMENDMENT TO CLAIMS

Please cancel claims 1-40 without prejudice.

Please add the following new claims 41-50:

41. A method for performing a cryptographic operation with resistance to external monitoring attacks, where said cryptographic operation includes performing a substitution operation using a predefined substitution table, said method comprising:
- (a) obtaining a representation of a predefined substitution table specifying a corresponding table value for each of a plurality of possible table index values;
  - (b) using random information, transforming said representation of said predefined substitution table into a new randomized representation of said substitution table;
  - (c) receiving a datum to be cryptographically processed;
  - (d) computing a blinded representation of a table index value from at least said datum;
  - (e) using said new randomized representation of said table, performing a substitution on said blinded table index value to derive a blinded representation of the table value corresponding to an unblinded version of said table index value in step (d); and
  - (f) using said blinded table value to compute a cryptographic result for use in securing a cryptographic protocol.

42. The method of claim 41, where said step (d) includes the substeps of:
- (i) obtaining an input masking parameter; and
  - (ii) deriving said blinded table index value from at least said input masking parameter and said received datum.

3.  
43. The method of claim ~~42~~<sup>2</sup>, where said blinded representation of said table value constitutes said unblinded version of said table value in step (e), exclusive-ORed with an output masking parameter whose value depends on said random information.

4.  
44. The method of claim ~~41~~<sup>1</sup>, where said transforming in step (b) includes permuting a plurality of entries in said predefined substitution table.

5.  
45. The method of claim ~~41~~<sup>1</sup>, where said transforming in step (b) includes computing at least one value in said randomized representation of said substitution table by exclusive-ORing at least one masking value with at least one value of said predetermined substitution table.

6.  
46. The method of claim ~~41~~<sup>1</sup>, where said transforming in step (b) includes representing said predefined substitution table as a plurality of tables.

7.  
47. A method for performing a cryptographic operation involving a substitution operation using a predefined substitution table, comprising:

- (a) obtaining random information;
- (b) using said random information, producing a randomized representation of said table;
- (c) receiving a datum to be cryptographically processed;
- (d) applying said randomized representation of said table to a table input derived from at least said datum to produce a substitution result randomized by said random information;

- (e) using said randomized substitution result, deriving a cryptographic result, where said cryptographic result is independent of said random information; and
- (f) using said cryptographic result as part of securing a cryptographic protocol.

8.  
48.

A device for performing a cryptographic operation, where said cryptographic operation involves a key and an input message and includes a substitution operation with a predefined substitution table, comprising:

- (a) a source of random data;
- (b) table randomization logic configured to use an output from said source of random data;
- (c) a memory for storing a randomized representation of a predefined substitution table;
- (d) table input parameter computation logic, configured to produce a table input parameter from at least a portion of an input message and said output from said source of random data;
- (e) first cryptographic computation logic configured to perform substitution operations on said table input parameter using said randomized representation of said predefined substitution table in said memory;
- (f) second cryptographic logic, configured to use said first cryptographic computation logic to compute a cryptographic result, where said cryptographic result depends solely on said key and said input message and is independent of said output from said source of random data.

9.  
49.

The device of claim 48 where said source of random data is a pseudorandom number generator.

10.  
50.

The device of claim 48 where said source of random data includes a source of truly random values.

A

**VERSIONS OF AMENDED CLAIMS  
WITH MARKINGS TO SHOW CHANGES MADE**

Claims 1-40 have been deleted.

New claims 41-50 have been added.

**\*\* Remainder of Page Is Intentionally Left Blank \*\***

FOUO - 081504  
9E60E66D

A